Herramientas de Criptoanálisis

Castro Lechtaler, Antonio[1, 2]; Cipriano, Marcelo[1]; García, Edith[1],
Liporace, Julio[1]; Maiorano, Ariel[1]; Malvacio, Eduardo[1]; Tapia, Néstor[1];

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Escuela Superior Técnica, Facultad de Ingeniería. Instituto Universitario del Ejército.
[2] CISTIC/FCE - Universidad de Buenos Aires.

acastro@est.iue.edu.ar , marcelocipriano@est.iue.edu.ar,
{edithxgarcia; jcliporace; maiorano; edumalvacio; tapianestor87}@gmail.com

RESUMEN.

Este proyecto persigue el estudio, analisis, desarrollo e implementación de técnicas o métodos criptográficos para ser aplicados a determinados generadores de secuencias seudoaleatorias tipo *Stream Ciphers*[1], en particular a aquellos algoritmos que involucran *LFSR´s*[2], *NLFSR´s*[3], *CCG*[4] y *CA*[5].

Se orientará el estudio a los métodos *Criptoanálisis Diferencial*[1-2], *Lineal*[3], *Algebraico, Guess-and-Determi-ne[4]* y una de las últimas técnicas criptológicas denominada *Cube Attack*[6] [5].

Desarrollar un conjunto de herramientas que permitan analizar algoritmos de cifrado, generadores de secuencias seudoaleatoria, primitivas criptológicas, protocolos de seguridad de la información, claves secretas de distintos criptosistemas.

Palabras Clave:
Criptología, Criptoanálisis. Stream Ciphers.

[1] Stream cipher: generadores seudoaleatorios conocidos también como generadores en flujo o cadena.
[2] Linear Feedback Shift Registers: registros de desplazamiento realimentados linealmente.
[3] Non Linear Feedback Shift Registers: registros de desplazamiento realimentados no linealmente.
[4] Clock Controlled Generators: generadores controlados por reloj.
[5] Cellular Automata: autómata celular.
[6] Presentado en el congreso EuroCrypt del año 2009 por sus autores: Itai Dinur y Adi Shamir.

CONTEXTO.

El *Grupo de Investigación en Criptología y Seguridad Informática (GICSI)* pertenece al *Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CriptoLab)* pertenece a los *Laboratorios de Informática (InforLabs)* de la *Escuela Superior Técnica "Gral. Div. Manuel N. Savio" (EST)*, dependiente de la *Facultad del Ejército, Universidad Nacional de la Defensa (UNDEF)*. El mismo se enmarca en el área de la carrera de grado de *Ingeniería en Informática* y del posgrado en *Criptografía y Seguridad Teleinformática* que se dictan en esta institución.

1. INTRODUCCIÓN.

En la actualidad, el desarrollo de las comunicaciones electrónicas, el uso masivo y generalizado de las computadoras, la transmisión y almacenamiento de grandes flujos de información, hace necesario tomar una serie de medidas para poder protegerlos manteniendo su confidencialidad, autenticidad e integridad.

Es entonces cuando la *Criptología* pasa a ser una exigencia, una necesidad real, donde la falta de protección de los datos privados pasa a ser una amenaza latente.

Los sistemas criptológicos o las primitivas criptográficas creadas para sortear diferentes amenazas deben ser cuidado-

sa y eficientemente desarrolladas y evaluadas. Al momento de realizar el diseño de un criptosistema se deben tener en cuenta todos los ataques que éste puede sufrir. Cada filosofía de diseño que se aplica está respondiendo a un hipotético procedimiento de criptoanálisis y así demostrar su resistencia a él.

Hoy en día no se puede hablar de una única modalidad general de criptoanálisis. Cada algoritmo, cada primitiva, cada protocolo debe ser atacado mediante una técnica adecuada a su estructura.

El criptoanálisis tiene un impacto significativo en el mundo real, puesto que los algoritmos criptológicos, los proto- colos y también los tamaños de las cla- ves entre otros, son seleccionados basándose en el estado del arte del criptoanálisis.

En los últimos años los métodos para el diseño de algoritmos seguros han tenido un gran avance e impulso a nivel mundial. Basta recordar, entre otros, los llamados en 1997 del *NIST*[7] para escoger un nuevo algoritmo como estándar de cifrado llamado AES [6]. El concurso europeo *e-Stream* en 2004, organizado por el *E-CRYPT* [7] del cual superaron todas las pruebas y ataques, 7 algoritmos: 4 para software y 3 para hardware. Y el concurso aún en proceso *CAESAR*[8] el cual se espera que este año 2017 emita el ganador o un portfolio de los algoritmos que lleguen al final de las etapas del certamen [8].

Aunque bienvenido, este renacimiento mundial por la búsqueda de nuevos algoritmos por sí sólo resulta insuficiente a la hora de establecer parámetros criptográficos seguros.

El objetivo fundamental del criptoanálisis es hallar las vulnerabilidades en uno o varios aspectos de la seguridad de los algoritmos criptológicos, implícita o explícitamente.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO.

Se ha dado en planificar este proyecto de investigación siguiendo 6 etapas:

1. Estado del Arte del Criptoanálisis de los Stream Ciphers. Mediante el estudio de bibliografía actualizada y oportunamente solicitada, así como la asistencia a Cursos, Congresos y Workshops específicos del área, se profundizará en el estado del arte del *Criptoanálisis de los Stream Ciphers* y los nuevos ataques que se han desarrollado en la comunidad criptológica mundial.
2. Estudio, análisis y selección de los generadores de secuencias cifrantes. A través del estudio de las distintas plataformas y entornos se seleccionarán algoritmos para aplicar las prácticas y métodos criptográficos.
3. Relevamiento de los métodos criptográficos que se analizarán. Ataque por Fuerza Bruta, Criptoanálisis Li- neal, Criptoanálisis Diferencial, Ata- que por Correlación, Cube Attack, Ataque Algebraico.
4. Estudio de técnicas criptográficas. Determinar el o los métodos adecuados a la estructura del algoritmo estudiado.
5. Implementación de los métodos de criptoanálisis. Desarrollar e implementar las técnicas de criptoanálisis aplicadas a determinados generadores.
6. Análisis de los resultados obtenidos. Evaluar los resultados obtenidos para poder establecer el grado de fortaleza del algoritmo elegido.

[7] Institución de Estados Unidos, llamada Instituto de Normas y Estandarización (National Institute of Standards and Technology) por sus siglas en inglés.
[8] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness.

3. RESULTADOS OBTENIDOS / ESPERADOS.

Como resultado de esta investigación se propone realizar el estudio y análisis para el desarrollo de técnicas y/o herramientas criptoanalíticas que posibiliten la realización del diseño de aplicaciones criptográficas, como así también su evaluación, determinar sus vulnerabilidades o si es posible, quebrarlas.

Los alcances del criptoanálisis podrán ser:

a- Obtención de la/s clave/s del cifrado.
b- Hallar patrones estadísticos en la salida del sistema estudiado.
c- Desarrollar nuevas técnicas criptoanalíticas de acuerdo a las propiedades del sistema estudiado.
d- Analizar el algoritmo de generación de la/s clave/s y estudiar su vulnerabilidad.

Para ello se perseguirán los objetivos particulares:

1- Estudio y análisis de técnicas criptoanalíticas.
2- Diseño y desarrollo de herramientas de evaluación, ataque o quiebre de aplicaciones criptográficas.
3- Pruebas y testeo de las herramientas desarrolladas sobre algoritmos específicos.

4. FORMACIÓN DE RECURSOS HUMANOS.

Los docentes investigadores de este proyecto se encuentran dictando las asignaturas *Matemática Discreta, Paradigmas de Programación I, II* y *Criptografía y Seguridad Teleinformática.* Desde allí se invita a los alumnos a participar en los proyectos de investigación que se llevan adelante. Es por ello que los alumnos *LEIRAS*, *F. MIGLIARDI A., MONTANARO, L. ROMERO, E. y UVIEDO, G.* han demostrado su interés y se han sumado en calidad de colaboradores.

El *Cap. Pérez, P.* integra el equipo de investigación desde el año 2015 y se espera que este año realice su Proyecto Final de Carrera en un tema afín con este proyecto de investigación.

Atendiendo a la responsabilidad ética y social que compete a la actividad científica y tecnológica, el Grupo Integrante de este Proyecto de Investigación, ya sea durante su ejecución o por la aplica- ción de los resultados obtenidos, desea expresar su compromiso a no realizar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio ambiente, a los animales y/o a las generaciones futuras.

5. BIBLIOGRAFÍA

[1] Ding C.; *The differential cryptanalysis and design of natural stream ciphers*. In: Anderson R. (eds.) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol. 809. Springer Berlin, Heidelberg.

[2] Wu H., Preneel B. *Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy*. In: Naor M. (eds.) Advances in Cryptology. EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515. Springer Berlin, Heidelberg. 2007.

[3] Muller F., Peyrin T. *Linear Cryptanalysis of the TSC Family of Stream Ciphers.* In: Roy B. (eds.) Advances in Cryptology - ASIACRYPT 2007. Lecture Notes in Computer Science, vol. 3788. Springer, Berlin, Heidelberg. 2005.

[4] Pasalic, E.; *On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers*; IEEE Transactions on

Information Theory. Vol. 55 Ed.7º, 2009.

[5] Dinur I., Shamir A. *Cube Attacks on Tweakable Black Box Polynomials.* Advances in Cryptology - EUROCRYPT 2009. Lecture Notes in Computer Science, vol 5479. Springer, Berlin, Heidelberg. 2009.

[6] Daemen, J.; Rijmen, V.*; The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer. New York. 2002.

[7] http://www.ecrypt.eu.org/stream/ Consultada el 10-3-17.

[8] https://competitions.cr.yp.to/caesar.html. Consultada el 10-3-17.